In the Claims

Applicant respectfully requests entry of the following amendments to the claims. Applicant has submitted a new complete claim set showing marked up claims with insertions indicated by underlining and deletions indicated by strikeouts and/or double bracketing.

Please amend pending claims 1, 2, 5, 6, 8, 9, 12 13 and 16 as noted below.
Please cancel claims 3, 4, 14 and 15 as noted below.

1. (Currently Amended) A method for a mobile ~~first~~ computing device to make authentication information available to a base ~~second~~ computing device, the method comprising:

creating authentication information, the authentication information including content data that include data for updating a care-of address of the mobile computing device, a public key of the ~~first~~ mobile computing device, a network address of the ~~first~~ mobile computing device, and a digital signature, the network address having a portion derived from the public key of the ~~first~~ mobile computing device, the digital signature generated by signing with a private key of the ~~first~~ mobile computing device corresponding to the public key, the digital signature generated from data in the set: the content data, a hash value of data including the content data; and

making the authentication information available to the base ~~second~~ computing device.

2. (Currently Amended) A method as in claim 1 wherein the authentication information is made available to the base ~~second~~ computing device by sending a message incorporating the authentication information to the ~~second~~ base computing device.

3. (Canceled)

4. (Canceled)

5. (Currently Amended) A method as in claim [[4]] 1, wherein the base ~~second~~ computing device is a home agent for the ~~first~~ mobile computing device, and wherein the network address of the ~~first~~ mobile computing device is a home address of the ~~first~~ mobile computing device.

6. (Currently Amended) A method as in claim [[4]] 1, wherein the ~~second~~ base computing device is a correspondent of the ~~first~~ mobile computing device, and wherein the network address of the ~~first~~ mobile computing device is a home address of the ~~first~~ mobile computing device.

7. A method as in claim 1, wherein the public key and the private key together form an uncertified key pair.

8. (Currently Amended) A method as in claim 1, wherein the network address of the ~~first~~ mobile computing device includes a route prefix portion and a node-selectable portion, and the node-selectable portion includes a portion of a hash value of data including the public key of the ~~first~~ mobile computing device.

9. (Currently Amended) A method as in claim 8, wherein the node-selectable portion includes a portion of a hash value of data including the public key of the ~~first~~ mobile computing device and a modifier selected for preventing address conflicts.

10. A method as in claim 1, wherein the authentication information further includes data for preventing a replay attack.

11. A method as in claim 10, wherein the data for preventing a replay attack are in the set: time stamp, data identifying the second computing device as an intended recipient of the authentication information.

12. (Currently Amended) A computer-readable medium containing instructions for performing a method for a first computing device to make authentication information available to a second computing device, the method comprising:

creating authentication information, the authentication information including content data that include data for updating a care-of address of the first computing device, a public key of the first computing device, a network address of the first computing device, and a digital signature, the network address having a portion derived from the public key of the first computing device, the digital signature generated by signing with a

private key of the first computing device corresponding to the public key, the digital signature generated from data in the set: the content data, a hash value of data including the content data; and

making the authentication information available to the second computing device.

13. (Currently Amended) A computer-readable medium having stored thereon a data structure, the data structure comprising:

content data that include data for updating a care-of address of a computing device;

a public key of the [[a]] computing device;

a network address of the computing device, the network address having a portion derived from the public key of the computing device; and

a digital signature, the digital signature generated by signing with a private key of the computing device corresponding to the public key, the digital signature generated from data in the set: the content data, a hash value of data including the content data.

14. (Canceled)

15. (Canceled)

16. (Currently Amended) A data structure as in claim [[15]] 13, wherein the network address of the computing device is a home address of the computing device.

17. A data structure as in claim 13, wherein the network address of the computing device includes a route prefix portion and a node-selectable portion, and the node-selectable portion includes a portion of a hash value of data including the public key of the computing device.

18. A data structure as in claim 17, wherein the node-selectable portion includes a portion of a hash value of data including the public key of the computing device and a modifier selected for preventing address conflicts.

19. A data structure as in claim 13, wherein the data structure further includes data for preventing a replay attack.

20. A method for a second computing device to authenticate content data made available by a first computing device, the method comprising:

accessing authentication information made available by the first computing device, the authentication information including the content

data, a public key of the first computing device, a first network address of the first computing device, and a digital signature;

deriving a portion of a second network address from the public key of the first computing device;

validating the digital signature by using the public key of the first computing device;

accepting the content data if the derived portion of the second network address matches a corresponding portion of the first network address and if the validating shows that the digital signature was generated from data in the set: the content data, a hash value of data including the content data.

21. A method as in claim 20, further comprising:

determining whether to accept the content data based on a time stamp in the authentication information.

22. A method as in claim 20, wherein the content data include data for updating a communications parameter for the first computing device, the method further comprising:

updating a record of a communications parameter for the first computing device.

23. A method as in claim 22, wherein the communications parameter is a care-of address of the first computing device, and wherein updating includes updating a routing table maintained by the second computing device.

24. A method as in claim 20, wherein the authentication information further includes a modifier, and wherein deriving includes appending the modifier to the public key of the first computing device before deriving a portion of the second network address.

25. A computer-readable medium containing instructions for performing a method for a second computing device to authenticate content data made available by a first computing device, the method comprising:

accessing authentication information made available by the first computing device, the authentication information including the content data, a public key of the first computing device, a first network address of the first computing device, and a digital signature;

deriving a portion of a second network address from the public key of the first computing device;

validating the digital signature by using the public key of the first computing device;

accepting the content data if the derived portion of the second network address matches a corresponding portion of the first network address and if the validating shows that the digital signature was generated from data in the set: the content data, a hash value of data including the content data.